IN THE CLAIMS:

1. (Currently Amended) A method for enabling integrity checking of a software module to be used in a mobile communication terminal, said terminal capable of communicating in a mobile communication system, said software module being stored on a removable memory unit connected to the terminal, ~~said method characterized in that~~wherein the terminal communicates via the mobile communication system with the software provider, said communication including reception of a digitally signed data block comprising a reference value for use during integrity checking of said software module.

2. (Currently Amended) A method according to claim 1, comprising ~~the steps of~~:

hashing the software module, resulting in a first hash value,

transmitting a first identifier, associated with the memory unit, a second identifier, associated with the terminal and the first hash value via the mobile communication system to a provider of the software module,

receiving, from the provider of the software module, a data block comprising a digital signature and further data associated with the memory unit and the terminal,

analyzing the received data block, comprising verification of the digital signature and comparison of said further data with said first and second identifiers,

storing the received data block comprising the digital signature, thereby providing a reference value for use during integrity checking of said software module.

3. (Original) A method according to claim 2, where the transmission of the first identifier includes transmission of a memory unit serial number.

4. (Original) A method according to claim 2, where the transmission of the first identifier includes transmission of a software module identification number.

5. (Original) A method according to claim 2, where the transmission of the second identifier includes transmission of an international mobile station equipment identity code.

6. (Currently Amended) A mobile communication terminal, comprising means for enabling integrity checking of a software module to be used in the terminal, said terminal capable of communicating in a mobile communication system, said software module being stored on a removable memory unit connected to the

terminal, said terminal ~~c h a r a c t e r i z e d in that it comprises~~comprising means for communicating via the mobile communication system with the software provider, said means for communication including means for receiving a digitally signed data block comprising a reference value for use in means for integrity checking of said software module.

7. (Original) A terminal according to claim 6, comprising:

means for hashing the software module, arranged to provide a first hash value,

means for transmitting a first identifier, associated with the memory unit, a second identifier, associated with the terminal and the first hash value via the mobile communication system to a provider of the software module,

means for receiving, from the provider of the software module, a data block comprising a digital signature and further data associated with the memory unit and the terminal,

means for analyzing the received data block, comprising means for verification of the digital signature and comparison of said further data with said first and second identifiers,

means for storing the received data block comprising the digital signature, arranged to provide a reference value for use during integrity checking of said software module.

8. (Original) A terminal according to claim 7, where the means for transmitting the first identifier includes means for transmitting a memory unit serial number.

9. (Original) A terminal according to claim 7, where the means for transmitting the first identifier includes means for transmitting a software module identification number.

10. (Original) A terminal according to claim 7, where the means for transmitting the second identifier includes means for transmitting an international mobile station equipment identity code.

11. (New) Apparatus, comprising:

signal processor for processing a software module in such a way as to carry out a hash calculation on said software module for providing a hash value signal; and

a transmitter, responsive to said hash value signal for transmitting same via a communication network to a server of a software provider of said software module wherein said transmitter is also for transmitting an international mobile station equipment identity code of said apparatus and a serial number of a memory unit on which said software module is stored along with said hash calculation in said hash value signal to said server.

12. (New) The apparatus of claim 11, further comprising a receiver, responsive to a key file signal from said server via said communication network, for providing same to said signal processor for verification of a signature of said server made on said key file, for checking an international mobile station equipment identity code sent back by said server is the same as that of said apparatus and for comparing a serial number of said memory unit sent back by said server with that of said memory unit currently installed in said apparatus for permitting said software module to execute in case said identity code and said serial number sent back by said server match the identity code of said apparatus and the serial number of said memory unit currently installed in said apparatus.

13. (New) The apparatus of claim 12, further comprising a memory within which to store said signal key file received from said server.

14. (New) Method, comprising:

checking whether a hash value signal received over a communication network from a terminal device matches a hash value of a software module provided by a software provider, and in case of a match,

signing identifying information received along with said hash value signal from said terminal identifying said terminal device and a memory unit in which said software module is stored, and

returning signed identifying information as a key file signal to said terminal device over said communication network.

15. (New) Apparatus, comprising:

means for checking whether a hash value signal received over a communication network from a terminal device matches a hash value of a software module provided by a software provider, and in case of a match,

means for signing identifying information received along with said hash value signal from said terminal identifying said terminal device and a memory unit in which said software module is stored, and

means for returning signed identifying information as a key file signal to said terminal device over said communication network.

16. (New) System, comprising:

a server comprising:

means for checking whether a hash value signal received over a communication network from a terminal device matches a hash value of a software module provided by a software provider, and in case of a match,

means for signing identifying information received along with said hash value signal from said terminal identifying said terminal device and a memory unit in which said software module is stored, and

means for returning signed identifying information as a key file signal to said terminal device over said communication network

terminal device, comprising:

signal processor for processing a software module in such a way as to carry out a hash calculation on said software module for providing a hash value signal; and

a transmitter, responsive to said hash value signal for transmitting same via a communication network to a server of a software provider of said software module.

17. (New) The system of claim 16, wherein said transmitter is also for transmitting an international mobile station equipment identity code of said apparatus and a serial number of a memory unit on which said software module is stored along with said hash calculation in said hash value signal to said server.

18. (New) The system of claim 17, wherein said terminal device further comprises a receiver, responsive to a key file signal from said server via said communication network, for providing same to said signal processor for verification of a signature of said server made on said key file, for checking an international mobile station equipment identity code sent back by said server is the same as that of said apparatus and for comparing a serial number of said memory unit sent back by said server with that of said memory unit currently installed in said apparatus for permitting said software module to execute in case said identity code and said serial number sent back by said server match the identity code of said apparatus and the serial number of said memory unit currently installed in said apparatus.

19. (New) The system of claim 18, wherein said terminal device further comprises a memory within which to store said signal key file received from said server.

20. (New) A method for enabling integrity checking of a software module to be used in a mobile communication terminal, said terminal capable of communicating in a mobile communication system, said software module already stored on a removable memory unit connected to the terminal and ready for use except, before allowing the software module to take control of the terminal, the terminal communicates via the mobile communication system with a software provider, said communication including transmitting by said terminal of identifying information concerning said terminal and said memory unit to said software provider and receiving by said terminal a digitally signed data block comprising a reference value for use during integrity checking of said software module and allowing the software module to take control of the terminal only if the integrity of the software module properly checks.

21. (New) The method of claim 20, comprising:

hashing the software module, resulting in a first hash value, wherein said transmitting of identifying information comprises transmitting a first identifier, associated with the memory unit, a second identifier, associated with the terminal

and the first hash value via the mobile communication system to said software provider,

receiving, from the software provider, a data block comprising a digital signature and further data associated with the memory unit and the terminal,

analyzing the received data block, comprising verification of the digital signature and comparison of said further data with said first and second identifiers, and

storing the received data block comprising the digital signature, thereby providing a reference value for use during integrity checking of said software module.

22. (New) Apparatus, comprising:

a device for enabling integrity checking of a software module to be used in a mobile communication terminal, said terminal capable of communicating in a mobile communication system, said software module already stored on a removable memory unit connected to the terminal and ready for use except, before allowing the software module to take control of the terminal, the terminal communicates via the mobile communication system with a software provider, said device including

a transmitter for transmitting identifying information concerning said terminal and said memory unit to said software provider and

a receiver for receiving a digitally signed data block comprising a reference value for use during integrity checking of said software module and allowing the software module to take control of the terminal only if the integrity of the software module properly checks.

23. (New) The apparatus of claim 22, further comprising:

a device for hashing the software module, resulting in a first hash value, wherein said transmitting of identifying information comprises transmitting a first identifier, associated with the memory unit, a second identifier, associated with the terminal and the first hash value via the mobile communication system to said software provider,

a device for receiving, from the software provider, a data block comprising a digital signature and further data associated with the memory unit and the terminal,

a device for analyzing the received data block, comprising verification of the digital signature and comparison of said further data with said first and second identifiers, and

a device for storing the received data block comprising the digital signature, thereby providing a reference value for use during integrity checking of said software module.